PRIVACY POLICY

NATIONAL UNIVERSITY OF SCIENCE AND TECHNOLOGY

2025

1 Contents

2 Policy Approval

#	DESIGNATION	NAME	AUTHORISED BY	SIGNATURE	DATE
1	**Reviewed by:**	ICT Senate Committee	ICT Senate Chairperson		
2	**Approved by:**	Senate	Senate Chairperson		
3	**Ratified by:**	University Council	Council Chairperson		

3 Introduction

The National University of Science and Technology (NUST) is committed to protecting the privacy and personal data of its students, staff, faculty, and all users of its Information and Communication Technology (ICT) resources. This Privacy Policy outlines how NUST collects, processes, stores, and protects personal data in compliance with the Cyber and Data Protection Act [Chapter 12:07] and other relevant University policies.

4 Purpose of this Policy

This policy aims to:

- Inform data subjects about how NUST handles their personal data.
- Ensure transparency in data processing activities.
- Uphold the rights of data subjects regarding their personal information.
- Detail NUST's commitment to data security and privacy.

5 Scope

This policy applies to all personal data processed by NUST, whether collected directly from data subjects or other sources, and covers all NUST ICT resources. It applies to:

- All NUST students (undergraduate and postgraduate)
- All NUST academic, administrative, and support staff
- Researchers and visiting scholars
- Any other individual who provides personal data to NUST or uses NUST ICT resources.

6 Definitions

- **Act:** Refers to the Cyber and Data Protection Act [Chapter 12:07].
- **Authority:** The Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ), designated as the Data Protection Authority.
- **Consent:** Any freely given, specific, informed, and unambiguous indication of

the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

- **Data Controller:** NUST, as the entity that determines the purposes and means of the processing of personal data.
- **Data Processor:** A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.
- **Data Subject:** An identified or identifiable natural person to whom personal data relates.
- **Personal Data:** Any information relating to an identified or identifiable natural person.
- **Processing:** Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- **Sensitive Information:** Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, data concerning health or sex life, genetic data, and biometric data.

7 Principles of Data Processing

NUST adheres to the following principles when processing personal data, as outlined in the Act:

- **Lawfulness, Fairness, and Transparency (Act, Section 13(b)):** Personal information is processed lawfully, fairly, and in a transparent manner in relation to the data subject.
- **Purpose Limitation (Act, Section 9(1)):** Data is collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- **Data Minimisation (Act, Section 7(1)(a)):** Data processed is adequate, relevant, and not excessive in relation to the purpose for which it is processed.
- **Accuracy (Act, Section 7(1)(b)):** Personal data is accurate and, where necessary, kept up-to-date. Every reasonable step is taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Storage Limitation (Act, Section 7(1)(c)):** Personal data is retained in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.
- **Integrity and Confidentiality (Act, Section 18):** Personal data is processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational

measures.

8 Collection and Use of Personal Data

NUST collects and uses personal data for various legitimate purposes related to its functions as an educational institution, including:

- **Academic Administration:** Admissions, registration, course enrollment, academic records, grading, graduation, and alumni relations.
- **Student Support:** Providing student services, accommodation, financial aid, health services, and disability support.
- **Human Resources:** Recruitment, employment, payroll, performance management, and staff development.
- **Research:** Conducting academic research (with appropriate ethical approvals and safeguards).
- **Campus Security:** Ensuring the safety and security of the University community and property.
- **ICT Services:** Providing access to network, email, learning management systems, and other digital resources.
- **Compliance:** Fulfilling legal and regulatory obligations.

9 Lawful Basis for Processing

NUST processes personal data based on one or more of the following lawful grounds:

- **Consent (Act, Sections 10, 11, 12):** Where the data subject has given explicit consent for specific purposes. For sensitive information (including genetic, biometric, and health data), written consent is generally required. Data subjects have the right to withdraw consent at any time, free of charge.
- **Contractual Necessity (Act, Section 10(3)(b)):** Processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- **Legal Obligation (Act, Section 10(3)(c)):** Processing is necessary for compliance with a legal obligation to which NUST is subject.
- **Vital Interests (Act, Section 10(3)(d)):** Processing is necessary to protect the vital interests of the data subject or of another natural person.
- **Public Interest (Act, Section 10(3)(e)):** Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in NUST.
- **Legitimate Interests (Act, Section 10(3)(f)):** Processing is necessary for the purposes of the legitimate interests pursued by NUST or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

10 Data Security and Protection Measures

NUST implements appropriate technical and organisational measures to ensure the security of personal data, protecting it against unauthorised or unlawful processing and against accidental loss, destruction, or damage (Act, Section 18; NUST Information Security Policy). These measures include:

- **Access Controls:** Strict controls on who can access personal data, based on the principle of least privilege and grant minimum privileges and access necessary to perform duties.
- **Role Based Access Controls**: Restrict data access based on job roles (e.g., faculty, admin, IT staff). Implementation of the Least Privilege Principle by granting the minimum necessary access to perform duties.
- **Encryption:** Use of encryption for sensitive data where appropriate, for data storage and backup use SHA512, AES-256, TLS/SSL.
- **Pseudonymisation:** Where feasible, processing personal data in a manner that it can no longer be attributed to a specific data subject without the use of additional information.
- **Confidentiality and Resilience:** Ensuring the ongoing confidentiality, integrity, availability, and resilience of processing systems and services.
- **Regular Testing:** Periodically testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of processing.
- **User Responsibilities (NUST ICT Acceptable Use Policy):** Users are responsible for maintaining the security of their accounts, including strong password practices and protecting against malware.
- **Email Security:** Implementation of email security measures, including blocking certain attachment types and appending disclaimers.
- **Physical security measures :** Access to the data centre will be restricted through biometric authentication.
- **Network & system security**: Use of firewalls & Intrusion Detection/Prevention Systems (IDS/IPS) to monitor and block unauthorised access.
- **User Authentication**: Require strong passwords, multifactor authentication (MFA), and periodic access reviews (disabling accounts of former employees, contractors and reviewing access levels).
- **Secure Storage**: Sensitive data will be stored in protected databases with firewalls and intrusion detection.
- **Regular Patching of software**: To keep software, OS, and security systems updated.
- The University will implement device tracking to minimise security/data breaches on mobile devices

11 Data Subject Rights

NUST respects the rights of data subjects as outlined in the Act (Section 14). These rights include:

- **Right to Access:** The right to obtain confirmation as to whether or not personal data concerning them is being processed, and, where that is the case, access to the personal data.
- **Right to Rectification:** The right to obtain the rectification of inaccurate personal data concerning them.
- **Right to Erasure ('Right to be Forgotten'):** The right to obtain the erasure of personal data concerning them without undue delay in certain circumstances.
- **Right to Restriction of Processing:** The right to obtain restriction of processing in certain circumstances.
- **Right to Data Portability:** The right to receive the personal data concerning them, which they have provided to NUST, in a structured, commonly used, and machine-readable format and have the right to transmit those data to another controller.
- **Right to Object:** The right to object, on grounds relating to their particular situation, to processing of personal data concerning them.
- **Rights in relation to Automated Decision Making (Act, Section 25):** The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them, unless legally justified.
- **Representation for Children and Incapacitated Individuals (Act, Sections 26 & 27):** A child data subject shall be represented by a competent person, and physically, mentally, or legally incapacitated data subjects shall be represented by a legally authorized person.

To exercise any of these rights, data subjects should contact the Data Protection Officer (DPO) using the contact details provided in Section 13.

12 Data Sharing and Disclosure

NUST may share personal data with third parties only under specific conditions:

- **With Consent:** When the data subject has given explicit consent for the sharing.
- **Legal Obligation:** When required by law (e.g., to law enforcement agencies, regulatory bodies).
- **Service Providers:** With trusted third-party service providers who perform functions on NUST's behalf (e.g., cloud hosting, IT support, payment processing), under strict contractual agreements that ensure data protection compliance.
- **Transborder Flow (Act, Sections 28 & 29):** Personal information may be transferred outside Zimbabwe only if the receiving country assures an adequate level of protection or if appropriate safeguards are in place as per the Act's regulations.

- NUST will not sell, rent, or lease personal data to third parties.

13 Data Retention

NUST retains personal data only for as long as necessary to fulfill the purposes for which it was collected, including for legal, accounting, or reporting requirements (Act, Section 7(1)(c)). Retention periods are determined based on the type of data, the purpose of processing, and legal obligations.

14 Security Breach Notification

In the event of a personal data security breach, NUST will act in accordance with the Act (Sections 19, 20, 21) and the Cyber and Data Protection (Licensing of Data Controllers and Appointment of Data Protection Officers) Regulations, 2024 (SI 155, Section 17). This includes notifying the Data Protection Authority without undue delay (within 24 hours if possible) if the breach is likely to result in a high risk to the rights and freedoms of data subjects.

15 Contact Information

For any questions, concerns, or requests regarding this Privacy Policy or the processing of your personal data, please contact NUST's Data Protection Officer:

Ms Novuyo N T Bobo

National University of Science and Technology (NUST)

ICTS Department

dataprotection@nust.ac.zw

+263719114467

Corner Gwanda Road and Cecil Avenue

Bulawayo

16 Policy Review

This policy will be reviewed yearly to ensure its continued relevance and compliance with evolving legal and regulatory requirements. However, in the event of significant changes in applicable laws, regulations, or legal interpretations (e.g., updates to the CDPA or national data protection laws), an immediate review and revision will be initiated to maintain compliance.

Last Update